SOME CONSEQUENCES OF THE KARPENKO-MERKURJEV THEOREM

AUREL MEYER[†] AND ZINOVY REICHSTEIN[††]

ABSTRACT. We use a recent theorem of N. A. Karpenko and A. S. Merkurjev to settle several questions in the theory of essential dimension.

1. INTRODUCTION

N. Karpenko and A. Merkurjev [KM] recently proved the following formula for the essential dimension of a finite p-group.

Theorem 1.1. *Let G be a finite p-group and k be a field of characteristic $\neq p$ containing a primitive pth root of unity. Then $\mathrm{ed}(G; p) = \mathrm{ed}(G) =$ the minimal value of $\dim(V)$, where the minimum is taked over all faithful linear k-representations $G \to \mathrm{GL}(V)$.*

The purpose of this paper is to explore some of the consequences of this theorem. We refer the reader to [BuR] or [JLY, Chapter 8] for background material on the essential dimension of a finite group, [BF] or [BRV₂] for the notion of essential dimension of a functor, and [Me] for a detailed discussion of essential dimension at a prime p. As usual, if the reference to k is clear from the context, we will sometimes write ed in place of ed_k.

The following notation will be used throughout.

For a finite group H, we will denote the intersection of the kernels of all multiplicative characters $\chi \colon H \to k^*$ by H'. In particular, if k contains an eth root of unity, where e is the exponent of H, then $H' = [H, H]$.

Given a p-group G, set $C(G)$ to be the center of G, $C(G)_p$ to be the p-torsion subgroup of $C(G)$. We will view $C(G)_p$ and its subgroups as $\mathbb{F}_p$-vector spaces, and write "$\dim_{\mathbb{F}_p}$" (or simply "$\dim$") for their dimensions. We further set

$$(1) \qquad K_i := \bigcap_{[G:H]=p^i} H' \quad \text{and} \quad C_i := K_i \cap C(G)_p \,.$$

for every $i \geq 0$, $K_{-1} := G$ and $C_{-1} := K_{-1} \cap C(G)_p = C(G)_p$.

Our first main result is following theorem. Part (b) may be viewed as a variant of Theorem 1.1.

Theorem 1.2. *Let G be a p-group, k be a field of characteristic $\neq p$ containing a primitive pth root of unity, and $\rho \colon G \hookrightarrow \mathrm{GL}(V)$ be a faithful linear representation of G. Then*

(a) ρ has minimal dimension among the faithful linear representations of G defined over k if and only if for every $i \geq 0$ the irreducible decomposition of ρ has exactly

$$\dim_{\mathbb{F}_p}(C_{i-1}) - \dim_{\mathbb{F}_p}(C_i)$$

irreducible components of dimension p^i, each with multiplicity 1.

(b) $\mathrm{ed}(G; p) = \mathrm{ed}(G) = \sum_{i=0}^{\infty}(\dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C_i)p^i$.

Note that $K_i = C_i = \{1\}$ for large i (say, if $p^i \geq |G|$), so only finitely many terms in the above infinite sum are non-zero.

We will prove Theorem 1.2 in section 2; the rest of the paper will be devoted to its applications. The main results we will obtain are summarised below.

Classification of p-groups of essential dimension $\leq p$.

Theorem 1.3. *Let p be a prime, k be a field of characteristic $\neq p$ containing a primitive pth root of unity and G be a finite p-group such that $G' \neq \{1\}$. Then the following conditions are equivalent.*

(a) $\mathrm{ed}_k(G) \leq p$,

(b) $\mathrm{ed}_k(G) = p$,

(c) The center $C(G)$ is cyclic and G has a subgroup A of index p such that $A' = \{1\}$.

Note that the assumption that $G' \neq \{1\}$ is harmless. Indeed, if $G' = \{1\}$ then by Theorem 1.2(b) $\mathrm{ed}(G) = \mathrm{rank}\,(G)$; cf. also [BuR, Theorem 6.1] or [BF, section 3].

Essential dimension of p-groups of nilpotency class 2.

Theorem 1.4. *Let G be a p-group of exponent e and k be a field of characteristic $\neq p$ containing a primitive e-th root of unity. Suppose the commutator subgroup $[G, G]$ is central in G. Then*

(a) $\mathrm{ed}_k(G; p) = \mathrm{ed}_k(G) \leq \mathrm{rank}\, C(G) + \mathrm{rank}\,[G, G](p^{\lfloor m/2 \rfloor} - 1)$, where p^m is the order of $G/C(G)$.

(b) Moreover, if $[G, G]$ is cyclic then $|G/C(G)|$ is a complete square and equality holds in (a). That is, in this case

$$\mathrm{ed}_k(G; p) = \mathrm{ed}_k(G) = \sqrt{|G/C(G)|} + \mathrm{rank}\, C(G) - 1\,.$$

Essential dimension of a quotient group. C. U. Jensen, A. Ledet and N. Yui asked if $\operatorname{ed} G \geq \operatorname{ed}(G/N)$ for every finite group G and normal subgroup $N \lhd G$; see [JLY, p. 204]. The following theorem shows that this inequality is false in general.

Theorem 1.5. *Let p be a prime and k be a field containing a primitive pth rooth of unity. For every real number $\lambda > 0$ there exists a finite p-group G and a central subgroup H of G such that $\operatorname{ed}_k(G/H) > \lambda \operatorname{ed} G$.*

Essential dimension of $\operatorname{SL}_n(\mathbb{Z})$. G. Favi and M. Florence [FF] showed that $\operatorname{ed}(\operatorname{GL}_n(\mathbb{Z})) = n$ for every $n \geq 1$ and $\operatorname{ed}(\operatorname{SL}_n(\mathbb{Z})) = n - 1$ for every odd n. For details, including the definitions of $\operatorname{ed}(\operatorname{GL}_n(\mathbb{Z}))$ and $\operatorname{ed}(\operatorname{SL}_n(\mathbb{Z}))$, see Section 5. For even n Favi and Florence showed that $\operatorname{ed}(\operatorname{SL}_n(\mathbb{Z})) = n - 1$ or n and left the exact value of $\operatorname{SL}_n(\mathbb{Z})$ as an open question. In this paper we will answer this question as follows.

Theorem 1.6. *Suppose k is a field of characteristic $\neq 2$. Then*

$$\operatorname{ed}_k(\operatorname{SL}_n(\mathbb{Z}); 2) = \operatorname{ed}_k(\operatorname{SL}_n(\mathbb{Z})) = \begin{cases} n - 1, & \text{if } n \text{ is odd,} \\ n, & \text{if } n \text{ is even} \end{cases}$$

for any $n \geq 3$.

Acknowledgement. Theorems 1.4(b) and 1.5(b) first appeared in the unpublished preprint [BRV$_1$] by P. Brosnan, the second author and A. Vistoli. We thank P. Brosnan and A. Vistoli for allowing us to include them in this paper. Theorem 1.4(b) was, in fact, a precursor to Theorem 1.1; the techniques used in [BRV$_1$] were subsequently strengthened and refined by Karpenko and Merkurjev [KM] to prove Theorem 1.1. The proof of Theorem 1.4(b) in Section 4 may thus be viewed as a result of reverse engineering. We include it here because it naturally fits into the framework of this paper, because Theorem 1.4(b) is used in a crucial way in [BRV$_2$], and because a proof of this result has not previously appeared in print.

2. Proof of Theorem 1.2

Throughout this section G will denote a p-group, and $C = C(G)_p$ will denote the p-torsion subgroup of the center of G. We will use the notations introduced in and just before the statement of Theorem 1.2. In particular,

$$K_{-1} = G \supset K_0 \supset K_1 \supset K_2 \supset \dots$$

will be the descending sequence of normal subgroups of G defined in (1) and $C_i = C \cap K_i$. We will repeatedly use the well-known fact that

(2)   A normal subgroup N of G is trivial if and only if $N \cap C$ is trivial.

We begin with three elementary lemmas.

Lemma 2.1. $K_i = \bigcap_{\dim(\rho) \leq p^i} \ker(\rho)$, *where the intersection is taken over all irreducible representations ρ of G of dimension $\leq p^i$.*

Proof. Let $j \leq i$. Recall that every irreducible representation ρ of G of dimension p^j is induced from a 1-dimensional representation χ of a subgroup $H \subset G$ of index p^j; cf. [Se, 8.16]. Thus $\ker(\rho) = \ker(\mathrm{ind}_H^G \chi) = \bigcap_{g \in G} g \ker(\chi)g^{-1}$, and since each $g \ker(\chi)g^{-1}$ contains $(gHg^{-1})'$, we see that $\ker(\rho) \supset K_j \supset K_i$. The opposite inclusion is proved in a similar manner. $\square$

Lemma 2.2. *Let G be a finite group over a field k that contains pth roots of unity. Let C be a central subgroup of exponent p and $\rho\colon G \to \mathrm{GL}(V)$ be an irreducible representation of G. Then*

(a) $\rho(C)$ consists of scalar matrices. In other words, the restriction of ρ to C decomposes as $\chi \oplus \ldots \oplus \chi$ ($\dim(V)$ times), for some multiplicative character $\chi\colon C \to \mathbb{G}_m$. We will refer to χ as the character associated to ρ.

(b) $C_i = \bigcap_{\dim(\rho) \leq p^i} \ker(\chi_\rho)$, where the intersection is taken over all irreducible G-representations ρ of dimension $\leq p^i$ and $\chi_\rho\colon C \to \mathbb{G}_m$ denotes the character associated to ρ.

In particular, if $\dim(\rho) \leq p^i$ then the associated character χ of ρ vanishes on C_i.

Proof. (a) Let $V = V_1 \oplus \cdots \oplus V_m$ be an irreducible decomposition of V as a direct sum of character spaces for C. That is, C acts on V_i by a multiplicative character χ_i, where $\chi_1, \ldots, \chi_m$ are distinct. Since C is central, each V_i is G-invariant. Since we are assuming that the representation of G on V is irreducible, this implies that $m = 1$, as claimed.

(b) By Lemma 2.1

$$C_i = C \cap \bigcap_{\dim(\rho) \leq p^i} \ker(\rho) = \bigcap_{\dim(\rho) \leq p^i} (C \cap \ker(\rho)) = \bigcap_{\dim(\rho) \leq p^i} \ker(\chi_\rho).$$

$\square$

Lemma 2.3. *Let G be a p-group and $\rho = \rho_1 \oplus \ldots \oplus \rho_m$ be the direct sum of the irreducible representations $\rho_i\colon G \to \mathrm{GL}(V_i)$. Let $\chi_i := \chi_{\rho_i}\colon C \to \mathbb{G}_m$ be the character associated to ρ_i.*

(a) ρ is faithful if and only if $\chi_1, \ldots, \chi_m$ span C^* as an $\mathbb{F}_p$-vector space.

(b) Moreover, if ρ is of minimal dimension among the faithful representations of G then $\chi_1, \ldots, \chi_m$ form an $\mathbb{F}_p$-basis of C^*.

Proof. (a) By (2), $\mathrm{Ker}(\rho)$ is trivial if and only if $\mathrm{Ker}(\rho) \cap C = \cap_{i=1}^m \mathrm{Ker}(\chi_i)$ is trivial. On the other hand, $\cap_{i=1}^m \mathrm{Ker}(\chi_i)$ is trivial if and only if $\chi_1, \ldots, \chi_m$ span C^*.

(b) Assume the contrary, say χ_m is a linear combination of $\chi_1, \ldots, \chi_{m-1}$. Then part (a) tells us that $\rho_1 \oplus \ldots \oplus \rho_{m-1}$ is a faithful representation of G, contradicting the minimality of $\dim(\rho)$. $\square$

We are now ready to proceed with the proof of Theorem 1.2. Part (b) is an immediate consequence of part (a) and Theorem 1.1. We will thus focus

on proving part (a). In the sequel for each $i \geq 0$ we will set

$$\delta_i := (\dim C_{i-1} - \dim C_i)$$

and

$$\Delta_i := \delta_0 + \delta_1 + \cdots + \delta_i = \dim(C) - \dim(C_i),$$

where the last equality follows from $C_{-1} = C$.

Our proof will proceed in two steps. In Step 1 we will construct a faithful representation μ of G such that for every $i \geq 0$ exactly δ_i irreducible components of μ have dimension p^i. In Step 2 we will show that $\dim(\rho) \geq \dim(\mu)$ for any other faithful representation ρ of G, and moreover equality holds if and only if for every $i \geq 0$ ρ has exactly δ_i irreducible components of dimension p^i.

Step 1: We begin by constructing μ. By definition,

$$C = C_{-1} \supset C_0 \supset C_1 \supset \ldots,$$

where the inclusions are not necessarily strict. Dualizing this flag of $\mathbb{F}_p$-vector spaces, we obtain a flag

$$(0) = (C^*)_{-1} \subset (C^*)_0 \subset (C^*)_1 \subset \ldots$$

of $\mathbb{F}_p$-subspaces of C^*, where

$$(C^*)_i := \{\chi \in C^* \,|\, \chi \text{ is trivial on } C_i\} \simeq (C/C_i)^*.$$

Let $\mathrm{Ass}(C) \subset C^*$ be the set of characters of C associated to irreducible representations of G, and let $\mathrm{Ass}_i(C)$ be the set of characters associated to irreducible representations of dimension p^i. Lemma 2.2(b) tells us that

$$\mathrm{Ass}_0(C) \cup \mathrm{Ass}_1(C) \cup \cdots \cup \mathrm{Ass}_i(C) \text{ spans } (C^*)_i$$

for every $i \geq 0$. Hence, we can choose a basis $\chi_1, \ldots, \chi_{\Delta_0}$ of $(C^*)_0$ from $\mathrm{Ass}_0(C)$, then complete it to a basis $\chi_1, \ldots, \chi_{\Delta_1}$ of $(C^*)_1$ by choosing the last $\Delta_1 - \Delta_0$ characters from $\mathrm{Ass}_1(C)$, then complete this basis of $(C^*)_1$ to a basis of $(C^*)_2$ by choosing $\Delta_2 - \Delta_1$ additional characters from $\mathrm{Ass}_2(C)$, etc. We stop when $C_i = (0)$, i.e., $\Delta_i = \dim(C)$.

By the definition of $\mathrm{Ass}_i(C)$, each χ_j is the associated character of some irreducible representation μ_j of G. By our construction

$$\mu = \mu_1 \oplus \cdots \oplus \mu_{\dim(C)},$$

has the desired properties. Indeed, since $\chi_1, \ldots, \chi_{\dim(C)}$ form a basis of C^*, Lemma 2.3 tells us that μ is faithful. On the other hand, by our construction exactly

$$\delta_i - \delta_{i-1} = \dim(C_i^*) - \dim(C_{i-1}^*) = \dim(C_{i-1}) - \dim(C_i)$$

of the characters $\chi_1, \ldots, \chi_c$ come from $\mathrm{Ass}_i(C)$. Equivalently, exactly $\dim(C_{i-1}) - \dim(C)$ of the irreducible representations $\mu_1, \ldots, \mu_c$ are of dimension p^i.

Step 2: Let $\rho \colon G \to \mathrm{GL}(V)$ be a faithful linear representation of G of the smallest possible dimension,

$$\rho = \rho_1 \oplus \ldots \oplus \rho_c$$

be its irreducible decomposition, and $\chi_i \colon C \to \mathbb{G}_m$ be the character associated to ρ_i. By Lemma 2.3(b), $\chi_1, \ldots, \chi_c$ form a basis of C^*. In particular, $c = \dim(C)$ and at most $\dim(C) - \dim(C_i)$ of the characters $\chi_1, \ldots, \chi_c$ can vanish on C_i. On the other hand, by Lemma 2.2(b) every representation of dimension $\leq p^i$ vanishes on C_i. Thus if exactly d_i of the irreducible representations $\rho_1, \ldots, \rho_c$ have dimension p^i then

$$d_0 + d_1 + d_2 + \ldots + d_i \leq \dim(C) - \dim(C_i)$$

for every $i \geq 0$. For $i \geq 0$, set $D_i := d_0 + \cdots + d_i =$ number of representations of dimension $\leq p^i$ among $\rho_1, \ldots, \rho_c$. We can now write the above inequality as

$$(3) \qquad\qquad\qquad D_i \leq \Delta_i \text{ for every } i \geq 0.$$

Our goal is to show that $\dim(\rho) \geq \dim(\mu)$ and that equality holds if and only if exactly δ_i of the irreducible representations $\rho_1, \ldots, \rho_{\dim(C)}$ have dimension p^i. The last condition translates into $d_i = \delta_i$ for every $i \geq 0$, which is, in turn equivalent to $D_i = \Delta_i$ for every $i \geq 0$.

Indeed, setting $D_{-1} := 0$ and $\Delta_{-1} := 0$, we have,

$$\dim(\rho) - \dim(\mu) = \sum_{i=0}^{\infty}(d_i - \delta_i)p^i = \sum_{i=0}^{\infty}(D_i - \Delta_i)p^i - \sum_{i=0}^{\infty}(D_{i-1} - \Delta_{i-1})p^i$$

$$= \sum_{i=0}^{\infty}(D_i - \Delta_i)(p^i - p^{i+1}) \geq 0\,,$$

where the last inequality follows from (3). Moreover, equality holds if and only if $D_i = \Delta_i$ for every $i \geq 0$, as claimed. This completes the proof of Step 2 and thus of Theorem 1.2. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

3. Proof of Theorem 1.3

Since $K_0 = G'$ is a non-trivial normal subgroup of G, we see that $K_0 \cap C(G)$ and thus $C_0 = K_0 \cap C(G)_p$ is non-trivial. This means that in the summation formula of Theorem 1.2(b) at least one of the terms

$$(\dim_{\mathbb{F}_p}(C_{i-1}) - \dim_{\mathbb{F}_p}(C_i))p^i$$

with $i \geq 1$ will be non-zero. Hence, $\mathrm{ed}(G) \geq p$; this shows that (a) and (b) are equivalent. Moreover, equality holds if and only if (i) $\dim_{\mathbb{F}_p}(C_{-1}) = 1$, (ii) $\dim_{\mathbb{F}_p}(C_0) = 1$ and (iii) C_1 is trivial. It remains to show that (i), (ii) and (iii) are equivalent to (c).

Since $C_{-1} = C(G)_p$, (i) is equivalent to $C(G)$ being cyclic.

Now recall that we are assuming $K_0 = G' \neq \{1\}$. By (2) this is equivalent to $C_0 = K_0 \cap C(G)_p \neq \{1\}$. Since $C_0 \subset C_{-1}$ has dimension at most 1, we see that (ii) follows from (i).

Finally, (iii) means that

$$(4) \qquad\qquad\qquad K_1 = \bigcap_{[G:H]=p} H'$$

intersects $C(G)_p$ trivially. Since K_1 is a normal subgroup of G, (2) tells us that (iii) holds if and only if $K_1 = \{1\}$.

It thus remains to show that $K_1 = \{1\}$ if and only if $H' = \{1\}$ for some subgroup H of G of index p. One direction is obvious: if $H' = \{1\}$ for some H of index p then the intersection (4) is trivial. To prove the converse, assume the contrary: the intersection (4) is trivial but $H' \neq \{1\}$ for every subgroup H of index p. Since every such H is normal in G (and so is H'), (2) tells us that that $H' \neq \{1\}$ if and only if $H' \cap C(G) \neq \{1\}$. Since $C(G)$ is cyclic, the latter condition is equivalent to $C(G)_p \subset H'$. Thus

$$C(G)_p \subset K_1 = \bigcap_{[G:H]=p} H',$$

contradicting our assumption that $K_1 \neq \{1\}$. □

4. Proof of Theorems 1.4 and 1.5

Proof of Theorem 1.4. Since the commutator $K_0 = [G,G]$ is central, $C_0 = K_0 \cap C(G)_p$ is of dimension $\operatorname{rank}[G,G]$ and the p^0 term in the formula of Theorem 1.2 is $(\operatorname{rank} C(G) - \operatorname{rank}[G,G])$.

Let $Q = G/C(G)$ which is abelian by assumption. Let $h_1, ..., h_s$ be generators of $[G,G]$ where $s = \operatorname{rank}[G,G]$, so that

$$[G,G] = \mathbb{Z}/p^{e_1} h_1 \oplus \cdots \oplus \mathbb{Z}/p^{e_1} h_1,$$

written additively. For $g_1, g_2 \in G$ the commutator can then be expressed as

$$[g_1, g_2] = \beta_1(g_1, g_2)h_1 + \ldots + \beta_s(g_1, g_2)h_s.$$

Note that each $\beta_i(g_1, g_2)$ depends on g_1, g_2 only modulo the center $C(G)$. Thus each β_i descends to a skew-symmetric bilinear form

$$Q \times Q \to \mathbb{Z}/p^{e_i}$$

which, by a slight abuse of notation, we will continue to denote by β_i. Let p^m be the order of Q. For each form β_i there is an isotropic subgroup Q_i of Q of order at least $p^{\lfloor (m+1)/2 \rfloor}$ (or equivalently, of index at most $p^{\lfloor m/2 \rfloor}$ in Q); see [AT, Corollary 3]. Pulling these isotropic subgroups back to G, we obtain subgroups $G_1, \ldots, G_s$ of G of index $\leq p^{\lfloor m/2 \rfloor}$ with the property that $G'_i = [G_i, G_i]$ lies in the subgroup of $C(G)$ generated by $h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_s$. In particular, $G'_i \cap \cdots \cap G'_s = \{1\}$. Thus, all K_i (and hence, all C_i) in (1) are trivial for $i \geq \lfloor m/2 \rfloor$, and Theorem 1.2 tells us that

$$\operatorname{ed}(G) = \dim_{\mathbb{F}_p} C_{-1} - \dim_{\mathbb{F}_p} C_0 + \sum_{i=1}^{\lfloor m/2 \rfloor} (\dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C_i)p^i \leq$$

$$\dim_{\mathbb{F}_p} C_{-1} - \dim_{\mathbb{F}_p} C_0 + \sum_{i=1}^{\lfloor m/2 \rfloor} (\dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C_i) \cdot p^{\lfloor m/2 \rfloor} =$$

$$\operatorname{rank} C(G) + p^{\lfloor m/2 \rfloor}(\operatorname{rank}[G,G] - 1).$$

(b) In general, the skew-symmetric bilinear forms β_i may be degenerate. However, if $[G, G]$ is cyclic, i.e., $s = 1$, then we have only one form, β_1, which is easily seen to be non-degenerate. For notational simplicity, we will write β instead of β_1. To see that β is non-degenerate, suppose $\overline{g} := g$ (modulo $C(G)$) lies in the kernel of β for some $g \in G$. Then by definition

$$\beta(g, g_1) = g g_1 g^{-1} g_1^{-1} = 1$$

for every $g_1 \in G$. Hence, g is central in G, i.e., $\overline{g} = 1$ in $Q = G/C(G)$, as claimed.

We conclude that the order of $Q = G/C(G)$ is a perfect square, say p^{2i}, and Q contains a maximal isotropic subgroup $I \subset Q$ of order $p^i = \sqrt{|G/C(G)|}$; see [AT, Corollary 4]. The preimage of I in G is a maximal abelian subgroup of index p^i. Consequently, $K_0 = [G, G], K_1, \ldots, K_{i-1}$ are all of rank 1 and K_i is trivial, where $p^i = \sqrt{|G/C(G)|}$. Moreover, since all of these groups lie in $[G, G]$ and hence, are central, we have $C_i = (K_i)_p$ and thus

$$\dim_{\mathbb{F}_p}(C_0) = \dim_{\mathbb{F}_p}(C_1) = \ldots = \dim_{\mathbb{F}_p}(C_{i-1}) = 1 \text{ and } \dim_{\mathbb{F}_p}(C_i) = 0.$$

Specializing the formula of Theorem 1.4 to this situation, we obtain part (b). $\qquad\square$

Example 4.1. Recall that a p-group G is called *extra-special* if its center C is cyclic of order p, and the quotient G/C is elementary abelian. The order of an extra special p-group G is an odd power of p; the exponent of G is either p or p^2; cf. [H, III. 13]. Note that every non-abelian group of order p^3 is extra-special. For extra-special p-groups Theorem 1.4(b) reduces to the following.

Let G be an extra-special p-group of order p^{2m+1}. Assume that the characteristic of k is different from p, that $\zeta_p \in k$, and $\zeta_{p^2} \in k$ if the exponent of G is p^2. Then $\operatorname{ed} G = p^m$.

Proof of Theorem 1.5. Let Γ be a non-abelian group of order p^3. The center of Γ has order p; denote it by C. Since Γ is extra-special, $\operatorname{ed}(\Gamma) = p$. (This also follows from Theorem 1.3.)

The center of $\Gamma^n = \Gamma \times \cdots \times \Gamma$ (n times) is then isomorphic to C^n. Let H_n be the subgroup of C^n consisting of n-tuples $(c_1, \ldots, c_n)$ such that $c_1 \ldots c_n = 1$. Clearly

$$\operatorname{ed} \Gamma^n \leq n \cdot \operatorname{ed}(\Gamma) = np;$$

see [BuR, Lemma 4.1(b)]. (In fact by [KM, Theorem 5.1], $\operatorname{ed} \Gamma^n = n \cdot \operatorname{ed}(\Gamma)$ but we shall not need this here.)

On the other hand, Γ^n / H_n, is easily seen to be extra-special of order p^{2n+1}, so $\operatorname{ed}(\Gamma^n / H_n) = p^n$ by Example 4.1. Setting $G = \Gamma^n$ and $H = H_n$, we see that the desired inequality $\operatorname{ed}(G/H) > \lambda \operatorname{ed} G$ holds for suitably large n. $\qquad\square$

5. Proof of Theorem 1.6

Recall that the essential dimension of the group $\mathrm{GL}_n(\mathbb{Z})$ over a field k, or $\mathrm{ed}_k(\mathrm{GL}_n(\mathbb{Z}))$ for short, is defined as the essential dimension of this functor

$$H^1(*, \mathrm{GL}_n(\mathbb{Z})) \colon K \to \{K\text{-isomorphism classes of } n\text{-dimensional } K\text{-tori}\},$$

where K/k is a field extension. Similarly $\mathrm{ed}_k(\mathrm{SL}_n(\mathbb{Z}))$ is defined as the essential dimension of the functor

$$H^1(*, \mathrm{SL}_n(\mathbb{Z})) \colon K \to \{K\text{-isomorphism classes of } n\text{-dimensional } K\text{-tori}$$
$$\text{with } \phi_T \subset \mathrm{SL}_n(\mathbb{Z}) \},$$

where $\phi_T \colon \mathrm{Gal}(K) \to \mathrm{GL}_n(\mathbb{Z})$ is the natural representation of the Galois group of K on the character lattice of T. The essential dimensions $\mathrm{ed}_k(\mathrm{GL}_n(\mathbb{Z}); p)$ and $\mathrm{ed}_k(\mathrm{SL}_n(\mathbb{Z}); p)$ are respectively the essential dimensions of the above functors at a prime p.

G. Favi and M. Florence [FF] showed that for $\Gamma = \mathrm{GL}_n(\mathbb{Z})$ or $\mathrm{SL}_n(\mathbb{Z})$,

$$(5) \qquad\qquad \mathrm{ed}(\Gamma) = \max\{\mathrm{ed}(F) | F \text{ finite subgroup of } \Gamma\}.$$

From this they deduced that

$$\mathrm{ed}(\mathrm{GL}_n(\mathbb{Z})) = n, \quad \text{and} \quad \mathrm{ed}(\mathrm{SL}_n(\mathbb{Z})) = \begin{cases} n - 1, \text{ if } n \text{ is odd,} \\ n - 1 \text{ or } n, \text{ if } n \text{ is even.} \end{cases}$$

For details, see [FF, Theorem 5.4].

Favi and Florence also proved that $\mathrm{ed}(\mathrm{SL}_2(\mathbb{Z})) = 1$ if k contains a primitive 12th root of unity and asked whether $\mathrm{ed}(\mathrm{SL}_n(\mathbb{Z})) = n - 1$ or n, in the case where $n \geq 4$ is even; see [FF, Remark 5.5]. In this section we will prove Theorem 1.6 which shows that the answer is always n.

A minor modification of the arguments in [FF] shows that (5) holds also for essential dimension at a prime p:

$$(6) \qquad\qquad \mathrm{ed}(\Gamma; p) = \max\{\mathrm{ed}(F; p) | F \text{ a finite subgroup of } \Gamma\},$$

where $\Gamma = \mathrm{GL}_n(\mathbb{Z})$ or $\mathrm{SL}_n(\mathbb{Z})$. The finite groups F that Florence and Favi used to find the essential dimension of $\mathrm{GL}_n(\mathbb{Z})$ and $\mathrm{SL}_n(\mathbb{Z})$ (n odd) are $(\mathbb{Z}/2\mathbb{Z})^n$ and $(\mathbb{Z}/2\mathbb{Z})^{n-1}$ respectively. Thus $\mathrm{ed}(\mathrm{GL}_n(\mathbb{Z}); 2) = \mathrm{ed}(\mathrm{GL}_n(\mathbb{Z})) = n$ for every $n \geq 1$ and $\mathrm{ed}(\mathrm{SL}_n(\mathbb{Z}); 2) = \mathrm{ed}(\mathrm{SL}_n(\mathbb{Z})) = n - 1$ if n is odd.

Our proof of Theorem 1.6 will rely on part (b) of the following easy corollary of Theorem 1.2.

Corollary 5.1. *Let G be a finite p-group, and k be a field of characteristic $\neq p$, containing a primitive pth root of unity.*

(a) If $C(G)_p \subset K_i$ then $\mathrm{ed}_k(G)$ is divisible by p^{i+1}.

(b) If $C(G)_p \subset G'$ then $\mathrm{ed}_k(G)$ is divisible by p.

(c) If $C(G)_p \subset G^{(i)}$, where $G^{(i)}$ denotes the ith derived subgroup of G, then $\mathrm{ed}_k(G)$ is divisible by p^i.

Proof. (a) $C(G)_p \subset K_i$ implies $C_{-1} = C_0 = \cdots = C_i$. Hence, in the formula of Theorem 1.2(b) the $p^0, p^1, \ldots, p^i$ terms appear with coefficient 0. All other terms are divisible by p^{i+1}, and part (a) follows.

(b) is an immediate consequence of (a), since $K_0 = G'$.

(c) By [H, Theorem V.18.6] $G^{(i)}$ is contained in the kernel of every p^{i-1}-dimensional representation of G. Lemma 2.1 now tells us that $G^{(i)} \subset K_{i-1}$ and part (c) follows from part (a). □

Proof of Theorem 1.6. We assume that $n = 2d \geq 4$ is even. To prove Theorem 1.6 it suffices to find a finite 2-subgroup F of $\mathrm{SL}_n(\mathbb{Z})$ of essential dimension n.

Diagonal matrices and permutation matrices generate a subgroup of $\mathrm{GL}_n(\mathbb{Z})$ isomorphic to $\mu_2^n \rtimes \mathrm{S}_n$. The determinant function restricts to a homomorphism $\det \colon \mu_2^n \rtimes \mathrm{S}_n \to \mu_2$ sending $((\epsilon_1, \ldots, \epsilon_n), \tau)) \in \mu_2^n \rtimes \mathrm{S}_n$ to the product $\epsilon_1 \epsilon_2 \cdot \ldots \cdot \epsilon_n \cdot \mathrm{sign}(\tau)$. Let P_n be a Sylow 2-subgroup of S_n and F_n be the kernel of

$$\det \colon \mu_2^n \rtimes P_n \to \mu_2 \, .$$

By construction F_n is a finite 2-group contained in $\mathrm{SL}_n(\mathbb{Z})$. Theorem 1.6 is now a consequence of the following proposition.

Proposition 5.2. *If* $\mathrm{char}(k) \neq 2$ *then* $\mathrm{ed}(F_{2d}) = 2d$ *for any* $d \geq 2$.

To prove the proposition, let

$$D_{2d} = \{\mathrm{diag}(\epsilon_1, \ldots, \epsilon_{2d}) \,|\, \text{each } \epsilon_i = \pm 1 \text{ and } \epsilon_1 \epsilon_2 \cdots \epsilon_{2d} = 1\}$$

be the subgroup of "diagonal" matrices contained in F_{2d}.

Since $D_{2d} \simeq \mu_2^{2d-1}$ has essential dimension $2d - 1$, we see that $\mathrm{ed}(F_{2d}) \geq \mathrm{ed}(D_{2d}) = 2d - 1$. On the other hand the inclusion $F_{2d} \subset \mathrm{SL}_{2d}(\mathbb{Z})$ gives rise to a $2d$-dimensional representation of F_{2d}, which remains faithful over any field k of characteristic $\neq 2$. Hence, $\mathrm{ed}(F_{2d}) \leq 2d$. We thus conclude that

$$(7) \qquad\qquad \mathrm{ed}(F_{2d}) = 2d - 1 \text{ or } 2d.$$

Using elementary group theory, one easily checks that

$$(8) \qquad\qquad C(F_{2d}) \subset [F_{2d}, F_{2d}] \subset F'_{2d} \, .$$

Thus $\mathrm{ed}(F_{2d})$ is even by Corollary 5.1; (7) now tells us that $\mathrm{ed}(F_{2d}) = 2d$. This completes the proof of Proposition 5.2 and thus of Theorem 1.6. □

Remark 5.3. The assumption that $d \geq 2$ is essential in the proof of the inclusion (8). In fact, $F_2 \simeq \mathbb{Z}/4\mathbb{Z}$, so (7) fails for $d = 1$.

Remark 5.4. Note that for any integers $m, n \geq 2$, F_{m+n} contains the direct product $F_m \times F_n$. Thus

$$\mathrm{ed}(F_{m+n}) \geq \mathrm{ed}(F_m \times F_n) = \mathrm{ed}(F_m) + \mathrm{ed}(F_n) \, ,$$

where the last equality follows from [KM, Theorem 5.1]. Thus Proposition 5.2 only needs to be proved for $d = 2$ and 3 (or equivalently, $n = 4$ and 6); all other cases are easily deduced from these by applying the above

inequality recursively, with $m = 4$. In particular, the group-theoretic inclusion (8) only needs to be checked for $d = 2$ and 3. Somewhat to our surprise, this reduction does not appear to simplify the proof of Proposition 5.2 presented above to any significant degree.

Remark 5.5. It is interesting to note that while the value of $\mathrm{ed}_k(\mathrm{SL}_2(\mathbb{Z}))$ depends on the base field k (see [FF, Remark 5.5]), for $n \geq 3$, the value of $\mathrm{ed}_k(\mathrm{SL}_n(\mathbb{Z}))$ does not (as long as $\mathrm{char}(k) \neq 2$).

References

[AT] A. Amitsur, J.P. Tignol, *Symplectic modules*, Israel J. Math. **54** (1986), 267-290.

[BF] G. Berhuy, G. Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279-330.

[BRV$_1$] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension and algebraic stacks*, 2007, `arXiv:math/0701903v1 [math.AG]`.

[BRV$_2$] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension, spinor groups and quadratic forms*, Annals of Math., to appear. Preprint available at
`http://annals.math.princeton.edu/issues/2008/FinalFiles/BrosnanReichsteinVistoliFinal.pdf`

[BuR] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159-179.

[FF] G. Favi, M. Florence, *Tori and essential dimension*, J. Algebra, **319** (2008), no. 9, 3885-3900.

[H] B. Huppert, Endliche Gruppen. I, Die Grundlehren der Mathematischen Wissenschaften, **134** Springer-Verlag, 1967.

[JLY] C. U. Jensen, A. Ledet, and N. Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, Cambridge, 2002, Constructive aspects of the inverse Galois problem.

[KM] N. A. Karpenko and A. S. Merkurjev, *Essential dimension of finite p-groups*, Inventiones Math., **172**, no. 3 (2008), pp. 491-508.

[Me] A. Merkurjev, *Essential dimension*, to appear in Proceedings of the International Conference on the algebraic and arithmetic theory of quadratic forms (Chile 2007), Contemporary Mathematics, American Mathematical Society, Providence, RI. Preprint posted at `http://www.math.ucla.edu/%7Emerkurev/publicat.htm`

[Se] J.-P. Serre, Linear representations of finite groups, Graduate Texts in Mathematics, **42**. Springer-Verlag, New York–Heidelberg, 1977.

Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada